UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/089,506	08/09/2002	William Henry Yost	RCA 89826	9456

7590 08/22/2006

Joseph S Tripoli
Thomson Multumedia Licensing
P O Box 5312
Princeton, NJ 08540

EXAMINER	
ABEDIN, SHANTO	
ART UNIT	**PAPER NUMBER**
2136	

DATE MAILED: 08/22/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/089,506	YOST, WILLIAM HENRY	
	Examiner	Art Unit	
	Shanto M Z Abedin	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *03* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *07 June 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-7* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-7* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This office action is in response to the communication filed on 06/07/2006.

2. The examiner would like to point out that this action is made **FINAL** (MPEP 706.07a).

3. The information disclosure statement received on 03/28/2002 had been considered, and a signed copy of the IDS had been sent to the applicant with the previous office action.

4. The examiner acknowledges that this application claim priority to a previous application filed on 09/28/1999.

5. Claim 1-7 are currently presented for the examination.

6. Claim 1-7 have been rejected.

Response to Arguments

7. Regarding claim 1-7, the applicant primarily argues that the reference Stallings does not teach:

(a)utilizing a deffi-hellman key exchange protocol by SNMP manager and the SNMP agent to enter an initial privacy key and an initial authentication key into the SNMPv3 device;

(b) reading by the SNMP manager, the public value of the SNMP agent through a SNMP request using an initial valid user having access to the public value of the SNMP agent; and

© wherein the public value of the SNMP manager is initially stored in a third entity different from that associated with the SNMP manager and the SNMP agent, and the method comprises downloading the configuration from the third entity by the SNMP agent.

8. In response to applicant's above argument (a)-(c) with respect to claim 1-7, they have been fully considered, but they are moot in view of the new ground(s) of rejection (see office action below).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claim 1-7 are rejected under 35 USC 103 (a) as being unpatentable over Stallings (SNMPv3: A Security Enhancement for SNMP, William Stallings, IEEE, 1998) in view of StJohns (Diffie-Hellman Key Change, Internet-draft, 1998).

Regarding claim 1, Stallings teaches a method for initializing a SNMP (simple network management protocol) v3 device using an SNMP agent in the SNMPv3 device and SNMP manager remote from the SNMPv3 device, comprising:

the SNMP manager and the SNMP agent to enter an initial privacy key and an initial authentication key into the SNMPv3 device (Page 11, Col 2 to Page 12, Col 2; key localization; authentication key; encryption/ key),

wherein said utilizing step includes:

generating an associated random number and public value by both the SNMP manager and the SNMP agent (Page 12, Col 1 to Page 13, Col 1; localized keys for agent; user keys; SHA-1; HMAC)

passing the public value of the SNMP manager to the SNMP agent in a configuration file (Page 13, Col 1, configuring localized key on agent's system in secure fashion);

reading by the SNMP manager, the public value of the SNMP agent through a SNMP request using an initial valid user having access to the public value of the SNMP agent (Page 12, Col 2, unique key for authorized users); and

computing a shared secret by the SNMP agent and the SNMP manager (Page 12, Col 2, shared secret key), wherein the method is characterized by the steps of :

converting the shared secret into a readable password (Fig 7, element: expended hashed password string; Page 12, Col 1, lines 29-48; human readable password; concatenating and repeating the users' password to itself to generate digest0; generating digest0 from the password; Page 12, Col 2, lines 29-40; "actual secret" shared between users and authoritative SNMP engine; single user's key; the examiner interprets such "expended password string" or "digest0" or "digest1" as claimed "readable password" because of their similar features);

converting the readable password into a secret key (Page 12, Col 1, lines 38-48; Page 12, Col 2, lines 29-40; localized keys; "secret key" shared by users and authoritative SNMP engine; converting users keys to unique keys; Page 13, Col 1, lines 1-12; the examiner interprets such "localized key" or "unique keys" or "secret keys" as claimed "secret keys" because of their similar features); and

setting the initial authentication key (Page 12, Col 1, lines 29-30; authentication key; Page 12, Col 2, lines 25-40; generating authentication key; Page 13, Col 1, lines 1-12; digest 2), and an initial privacy key to the value of the secret key (Page 12, Col 1, lines 29-30; privacy key; Page 12, Col 2, lines 25-40; generating encryption key).

Stallings fails to disclose utilizing a Diffie-Hellman key exchange protocol by the SNMP manager and the SNMP agent to enter an initial privacy key and an initial authentication key into the SNMPv3 device; and

computing a shared secret by the SNMP agent and the SNMP manager (Page 12, Col 2, shared secret key), using the Diffie Hellman key exchange protocol.

However, StJohns teaches utilizing a Diffie-Hellman key exchange protocol by the SNMP manager and the SNMP agent to enter an initial privacy key and an initial authentication key into the SNMPv3 device (Page 4, section 1.1 to Page 5, line 2); and

computing a shared secret by the SNMP agent and the SNMP manager (Page 12, Col 2, shared secret key), using the Diffie Hellman key exchange protocol (Page 7; shared secret).

StJohns and Stallings are analogous art because they are from the same field of endeavor of key management in SNMP. At the time of the invention it would have been obvious to a person of ordinary skill in art to combine the teachings of StJohns with Stallings to utilize a Diffie Hellman key exchange protocol for creating privacy keys, authentication keys, and shared secret keys in order to incorporate a commonly used network key agreement/ generation scheme such as Diffie Hellman protocol in MIB for providing further key security (StJohns, Page 1, 4).

Regarding claim 2, it is rejected applying as above rejecting claim 1, furthermore, Stallings teaches the method wherein the readable password comprises a 16 character password (Page 12, Col 1, lines 28-37; human-readable passwords; RFC-2274 algorithm for mapping password to key; octet privacy and authentication key; mapping password to key; Page 12, Col 2, lines 25-40; single/ plurality of password to create keys of plurality of bit length; *Stallings implies that such password can be eight or sixteen or any other suitable characters long depending on the level of security, and plurality of shorter password can be concatenated to create a longer password).*

Regarding claim 3, it is rejected applying as above rejecting claim 1, furthermore, Stallings teaches the method wherein the secret key comprises a 16 byte string (Page 12, Col 1, lines 29-49; Page 13, Col 1, lines 1-10; 16 octet key).

Regarding claim 4, it is rejected applying as above rejecting claim 1, furthermore, Stallings teaches the method further characterized in the configuration file comprises a proprietary

configuration file element for passing the public value of the SNMP manager to the SNMP agent (Page 3,Col 2, lines 26- 34; set of documents defining network protocol; proprietary network management applications; Page 4,Col 2, lines 25-50; Page 9,Col 2, lines 58-66; command generator; USM files in the security related parameters; authoritative module).

Regarding claim 5, it is rejected applying as above rejecting claim 4, furthermore, Stallings teaches the method wherein the SNMPv3 device operates in a SNMPv1/ v2c enabled network comprising a SNMPv2c device (Page 2, Col 2, lines 1-37; SNMPv3 defines a security capability to be used in conjunction with SNMPv2 or SNMPv1), and wherein the proprietary configuration file element is ignored by the SNMPv2c device (Fig 1, element : PDU processing for SNMPv1 or SNMPv2, element: SNMPv3 USM; Table 2, element: snmpSecurityModel; Page 2, Col 2, lines 5-35; User Security Model (USM) for SNMPv3; SNMP Protocol Data Unit (PDU) for SNMPv1 and SNMPv2; Page 3, Col 2, lines 25-45; Management Information Base (MIB) for keeping local configuration data for SNMPv2; *Stallings teachings of plurality of independent configuration/ security or management protocol for the different version of SNMP implies that the proprietary configuration file element used by SNMPv3 device can be ignored by the SNMPv2c device).*

Regarding claim 6, it is rejected applying as above rejecting claim 1, furthermore, StJohns discloses the method wherein the public value of the SNMP manager is included in a management information base (MIB) object in the configuration file (Page 7; usmDHPublicobjects).

Regarding claim 7, it is rejected applying as above rejecting claim 1, furthermore, StJohns discloses the method wherein the public value of the SNMP manager is initially stored in a third entity

different from that associated with the SNMP manager and the SNMP agent (Page 1, MIB, Agent , manager), and the method comprises downloading the configuration from the third entity by the SNMP agent (Page 9-10; usmUserPrivProtocol; usmDHKeyMIBCompliance; read; installed).

Conclusion

10. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL.** See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for response to this action is set to expire in 3 (Three) months and 0 (Zero) days from the mailing date of this letter. Failure to respond within the period for response will result in ABANDOMENT of the application (see 35 U.S.C 133, M.P.E.P 710.02(b)).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Shanto M Z Abedin whose telephone number is 571-272-3551. The examiner can normally be reached on M-F from 9:00 AM to 5:30 PM. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Moazzami Nasser, can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Shanto M Abedin

Examiner AU 2136

NASSER MOAZZAMI
PRIMARY EXAMINER

8/18/06